On the inability of existing security models to cope with data mobility in dynamic organizations

Trajce Dimkov, Qiang Tang, Pieter Hartel
{trajce.dimkov,qiang.tang,pieter.hartel}@utwente.nl

September 15, 2008

Abstract

Modeling tools play an important role in identifying threats in traditional IT systems, where the physical infrastructure and roles are assumed to be static. In dynamic organizations, the mobility of data outside the organizational perimeter causes an increased level of threats such as the loss of confidential data and the loss of reputation. We show that current modeling tools are not powerful enough to help the designer identify the emerging threats due to mobility of data and change of roles, because they do not include the mobility of IT systems nor the organizational dynamics in the security model. Researchers have proposed security models that particularly focus on data mobility and the dynamics of modern organizations, such as frequent role changes of a person. We show that none of the current security models simultaneously considers the data mobility and organizational dynamics to a satisfactory extent. As a result, none of the current security models effectively identifies the potential security threats caused by data mobility in a dynamic organization.

1 Introduction

In the last decade three main trends have emerged in the use of information systems. The first is information omnipresence raised by the increasing usage of mobile devices. The second trend is the increasing usage of outsourcing. Organizations gain access to highly trained workforce by becoming decentralized and by outsourcing whole business processes and departments. The last trend is the increasing cooperation between organizations. To increase market share, organizations carry out joint projects with other organizations and extensively hire part-time consultants.

Information omnipresence increases the risk of attacks that include physical tampering with mobile devices. Outsourcing and networked organizations are dynamic, making the distinction of roles in an organization difficult to define and maintain, which leads to increased risk from social engineering attacks [1].

Researchers from the industry are aware of the increase of mobility and the impact mobility has on security [2, 3, 4]. A number of mechanisms, such as best practices of protecting against laptop theft and protecting information in laptops are proposed to help the organization mitigate the threats due to mobility [23, 24, 25, 26]. All of the solutions partially restrict the data mobility and are based on best practice criteria.

Problem Information omnipresence, outsourcing and cooperation between organizations increase data mobility and role changes more than ever, making it increasingly difficult to secure the data.

Contribution We show that threats that arise from mobility of data in dynamic organization cannot be presented with the existing security modeling techniques. We define the requirements for an integrated security model and look in the literature at alternative models of the world that can represent the mobility of data in a dynamic organization. We analyze state of the art security models using attack scenarios presented in a case study, show that none of the new security models consider both of data mobility and organizational dynamics to a satisfactory extent, and present requirements for an integrated model that addresses this deficiency.

The remainder of the paper is organized as follows. Section 2 provides a case study of current threats that include mobility of objects, interaction between a person with a machine and interaction between two people. Section 3 introduces the requirements for an integrated security model of the world that is able to present the attacks presented in the case study. Section 4 presents the analysis of current models and shows to which extent the security models satisfy the requirements of the integrated security model. Section 5 concludes the paper.

2 Case study

To provide a focus for the analysis, we present a laptop case study. The first type of attack is based on permanent physical possession of the laptop and focuses on the confidentiality of the data stored inside. The second type of attack introduces social engineering as a way to provide access to the laptop and focuses on the integrity of the data in the laptop.

2.1 Confidentiality of the data in a laptop

If the adversary is in possession of the laptop, the adversary is also in possession of the encryption keys, making the storage of encryption keys in tamper resistant hardware crucial. The threat model of a storage device [5, 6] provides a variety of options for the adversary to consider, such as removal or tampering with parts of the device. The need for a good protection of the encryption keys has become widely acknowledged after the coldboot attack [7], which is therefore worthy of further study.

To present the coldboot attack, we first introduce a simplified example of presenting encrypted data to a user as shown in Figure 1. The snapshot is taken

from the Microsoft Threat and Analysis Modeling tool (TAM) and modified (e.g. numbers are added to present the sequence of the calls), to give a better overview of the example. The user presents to the operating system a key coupled with a

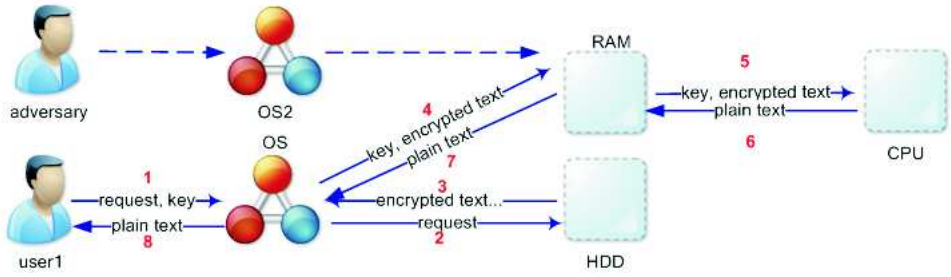

Figure 1: Coldboot attack

request that defines the data the user wants to read (1). The operating system forwards the request to the hard drive (2) and recovers the encrypted data (3). Then, the encrypted data together with the key is loaded into the RAM (4). From the RAM the data is fed into the processor (5), which as a result returns the plain text (6). The plain text is then sent to the user through the operating system (7,8). In the coldboot attack, the adversary does not target the hard drive with the sensitive information, but the RAM where the encryption keys are stored. When it is not possible to boot the computer from another media, the adversary physically transfers the RAM to another computer, and dumps the memory on a hard drive. Later, the adversary has all the time needed to use search algorithms on the dumped memory to get the encryption keys.

2.2 Rootkit attacks on a laptop using social engineering

Stealing a laptop provides an instantaneous benefit to the adversary. However, installing malware that sends data periodically from the internal network of the organization to the adversary is more dangerous. To infect the network, the adversary needs to combine social engineering with malicious software such as rootkits[27], making the mobile device an excellent carrier of the malicious software. There are several ways an adversary can use to install a rootkit [27] on a laptop. The term road apple refers to an apple that is found on a road, tempting the finder to take it. In the IT world, the apple is usually an infected generic dongle(ex. USB stick) with the logo of the organization left by the adversary in a social place of the organization, such as a cafeteria. When an employee finds the dongle he may be tempted to plug the dongle into his laptop [28]. In the rest of the paper we call this case road apple 1.

Another approach by the adversary to realize the road apple attack is through direct interaction with the employee. For example, the adversary impersonates higher level management and builds a trust relationship with the employee. The adversary provides a fake identity and simulates an emergency, asking to send

a file he has on a dongle through the laptop of the employee. If the employee plugs the dongle on the laptop, the dongle will install the rootkit without the employee's knowledge [8].In the rest of the paper we call this case road apple 2.

3 Integrated security model of the world

When an adversary tries to compromise a system, the adversary uses all available resources, which besides digital penetration include physical possession of a device and usage of social means to acquire sensitive information. To model the coldboot attack and physical tampering with devices, we need to be able to model the tamper resistance of components in a laptop. We also need to present the removal/addition of components in the laptop. The road apple attack, as many other social engineering attacks [1] relies on activities occurring in the digital, physical and social world. Thus, we need a model which presents movement and roles, as well as physical and digital objects.

The digital, social and physical aspects are defined by Wieringa [9] and we quote his definitions below:

> The physical world is the world of time, space, energy and mass measured by kilograms, meters, second, Amperes, etc. The social world is the world of conventions, money, commercial transactions, business processes, job roles, responsibility, accountability, etc. structured in terms of conceptual models shared by people. At the interface between the social and physical worlds we have the digital world which consists of symbols that have a meaning for people.

Here we provide requirements of an integrated security model of the world from the digital, social and physical aspect, together with the basic building blocks the model needs to include.

The requirements we want an integrated security model to achieve are:

1. *The model should be capable of representing the data of interest.*
2. *The model should be capable of representing the physical objects in which the data resides.*
3. *The model should be capable of representing the roles a user can have.*
4. *The model should define the interactions between the data, physical objects and the roles.*

The first three requirements present the digital, physical and social aspect of the world, while the last binds them together. Following the requirements and the definitions of the physical, digital and social aspect, elements of interest in the integrated security model are: *data*, *physical objects*, *roles* and *interaction relations*.

From the digital aspect represented by the data, we believe that the integrated model needs to present the data at rest as well as data in movement. The

spatial/temporal characteristic provides information about the movement of the objects which is needed to model the attacks presented in Section 2. To present tampering with a device, the model should be capable of presenting the physical properties of an object including the boundary of the object. From the social aspect we are interested in the transition of one role to another, as well as the interaction between roles. Through role interaction and role transition we can represent the impersonation of an adversary and adversary's direct interaction with an employee as presented in Section 2.2.

A model that will enable a security expert to observe the level of security of mobile data in dynamic organizations will give the security expert better insight in the threats and attack vectors, leading to an understanding of what kind of threat mitigation the security expert needs to implement. An integrated security model of the world will be a testbed for the effectiveness of the proposed mitigations.

To predict the behavior of a system over time we need a state based model. Schneider [10] argues that a static model cannot enforce security policies because the capability of a user can change over time. Goguen [11] presents a capability state model to present dynamic changes in the system, and based on the changes of the capability of a user, defines dynamic security policies. Goguen uses predicates defined over the sequences of operations used to reach the current state, instead of using a predicate on a single state.

4 Security models

Motivated by the examples of attacks described in section 2 we did an exhaustive literature search for models that are capable of presenting the attacks from the case study. The list of models we present here is not exhaustive due to the page limit. However, the models that we could not present fully are briefly discussed in the related work section. Most of the models we found focus on modeling the data from the digital aspect (e.g. data flow) and only a limited number of models consider the location of the data. To the best of our knowledge there is no integrated security model which includes all three aspects (digital, physical, social), and thus there is no model that can truthfully represent the security implications on data mobility in dynamic organizations.

We focus on models from the computer science domain modeling a security property of the system, such as privacy or confidentiality. TAM and Secure Tropos (ST) (Subsection 4.1) are static and used in the software industry for generation of threats for a specific software application. Then we move into dynamic, state based security models (Subsections 4.3 and 4.4) that include mobility of the components in the system. These dynamic models are all inspired by the ambient calculus [12], for which we provide the basic structure. Later we explore how ambient calculus is extended to focus on different properties of the world in two other security models. We analyze the characteristics of these models with respect to the requirements presented in section 3. A detailed analysis is presented in the extended version of the report [13].

4.1 TAM and Secure Tropos

One of the first steps when looking at a security issue is to create a threat model [14]. To generate the threats, the threat model needs to provide a security model of the system on which it runs the threat generation algorithm. Here we consider TAM [29] which is a state of the art tool used for internal threat generation and analysis in software development organizations, as well as Secure Tropos, a formal model used for high level presentation of software requirements.

In Figure 1 we use the TAM to model the coldboot attack. Besides being able to model data structures and data flow the tool also presents physical objects as well as roles. TAM considers the physical component and the role as static and the data as dynamic, allowing the TAM threat generation algorithm to focus on the flow of data. Although this reasoning is understandable and valid in software modeling, in the presented attacks TAM proves to be restrictive. TAM does not take into consideration the possibility that a component can be removed, such as the RAM in the coldboot attack nor that a component is mobile, such as the dongle in the road apple attack.

TAM presents neither role interaction nor role transition. Because of the lack of states, even with manipulation of the relationships and entities in the model, TAM cannot present interaction between roles and role transition. The role in TAM is used to describe the privileges over a component in an access control table, but does not define transition between roles such as escalation of privileges between a normal and an administrator role nor any interaction between roles, such as delegation or separation of duty. As a result, TAM cannot present the road apple attack where the adversary has direct interaction with the employee.

TAM cannot present physical properties of a component. A component is defined through the service type the component provides and the data and roles the component interacts with. Since TAM does not consider the component as a physical object, the component's resistance to physical attacks cannot be expressed in the model.

We can change the meaning of the components to present the attacks from the case study, but not without changing or blurring the relationship between the components. We can "attach" a new operating system to the RAM. As the number of mobile components increases the number of such "attachments" also increases, degrading the model usability as well as blurring the meaning of the relationship between components. Still TAM model "attachments" are used in modeling the coldboot attack as presented in Figure 1.

A similar approach is used in Secure Tropos[20], a formal model based on the static notions of ownership, trust and delegation. Secure Tropos is not state based, inheriting the same limitations as TAM, such as inability of dynamic change of roles and role interactions. Secure Tropos does not present spatial information, disabling the model to present physical threats such as tampering or mobility.

4.2 Ambient calculus

Ambient calculus [12] provides an excellent apparatus for modeling a world with mobile components. The calculus is capable of presenting spatial and temporal properties of a component(with running processes inside) in the model and is Turing complete. Ambient calculus serves as an inspiration for the state of the art security models that consider mobility of components.

Ambient calculus does not define the properties of an entity nor the relationship between entities, making the calculus generic enough to present any model of interest. The calculus presents a comprehensive theoretical framework for reasoning about mobility. But, without additional formal naming convention and definition of the properties of interest in the component, cannot be directly implemented in any model on which mechanisms such as policies or threat generation algorithms need to be applied.

Ambient calculus cannot present tampering with a device. In ambient calculus data decides to leave the device or not based on the capability of the data, which is not the case when an adversary tampers with a device. Although tamper resistance can be presented through a stack of ambients, the manipulation of the stack cannot be done at run time, because any rearrangement or removal of a layer requires a dynamic change of the capabilities of the data inside.

4.3 Scott's model

Scott [15] builds a security model of the world by addinga spatial relationship between the elements in the ambient calculus. Scott's model is based on a building block called an *entity*. An entity is a spatial location. Every entity belongs to only one of six defined *sorts*. To distinguish physical entities from digital entities, Scott defines a *context*, a physical/virtual machine capable of running code. Scott's model uses capabilities from ambient calculus (*in/out*) and renames the capabilities depending on which entity uses the capability. If the entity is a person moving between rooms, the capabilities are *walk in/walk out*. If the entity is a person interacting with a laptop, the capability is *pick up/put down*. If the entity is an agent moving between contexts, the capabilities are *emit/receive*.

To present tamper resistance of an entity, we can add multiple layers of protection to the data by inserting additional entities. But the definition of the *emit/receive* command teleports an entity from source address to destination address without taking in account the layers in between, making the model oblivious to the tamper resistance imposed by the device.

There is no social factor in the model of Scott. There is a sort `person`, but the meaning is spatial. The only capability this entity has is to pick up or put down a mobile entity. Through this we could present the coldboot attack, where the person physically changes the location of the RAM as well as the first version of the road apple attack. But the model cannot represent the direct interaction between the adversary and the employee in the second version of the road apple attack, where the adversary directly interacts with the employee

and convinces the employee to insert the dongle. Thus, the model cannot fully present the road apple attack.

4.4 Dragovic's model

Dragovic [16] presents a security model of the world by expanding Scott's model and focusing on exposure treats. The main building blocks are *data object*, which presents a collection of data with equal sensitivity as determined by a security policy and *container*, which is an ambient (digital or physical) containing a data object or a lower level container. In a Dragovic model, the container has as a boundary that protects the container or data object inside from the outside influences with variable degree of success. Every container propagates downwards its own influences in addition to the influences the container inherits from the parent container. Boundary transparency is defined based on the degree of protection the parent container offers to the child container. Dragovic uses *class* (similar to Scott's sort) to group elements. Another distinction is made by adding a *type* to the container, which presents the behavior of the container when exposed to an influence from the environment. Mobility of the data is presented by four operations: *enter*, *leave*, *migrate*, which atomically binds the previous two operators and *state_ update*, which is used to update the status of the attributes of a container. The model presented by Dragovic [17, 16] besides considering the spatial/temporal characteristics of the object, considers the object's physical properties, such as the object's capability to resist influences from the surrounding environment, making the model suitable for presenting the tamper resistance of a device.

The model of Dragovic includes Scott's model with the addition of the physical property of the objects, as well as the definition of sensitivity of data, allowing us to model tampering with a device and the coldboot attack to a level where all elements are realistically presented. When modeling the coldboot attack, we define the RAM as a container and the encryption key as a data object. The accessibility of the RAM is defined by the RAM's transparency in addition of the laptop's transparency. Before the coldboot attack, we consider the RAM as a container with limited tamper resistance. After the RAM is removed from the laptop, the tamper resistance of the RAM increases due to the degradation of the data. Thus, we can successfully present the coldboot attack.

Dragovic does not define an object *person*, therefore there is no defined interaction between a person and a container. By presenting the employee and the adversary as containers, we are able to present the movement of the dongle with the rootkit from the adversary to the employee's laptop. Yet, we are not able to present the interaction between the adversary and the employee, where the employee is convinced to insert the dongle. Thus, we cannot model the road apple attack with direct interaction.

4.5 Comparison of the models

This section compares the analyzed modeling approaches. Table 1 presents the objects and properties of the objects we are interested in the analyzed models.

Aspect	Element	Property	TAM & ST	Ambient calculus	Scott	Dragovic
Digital	Data	static	yes	yes	yes	yes
		dynamic	yes	yes	yes	yes
Physical	Ovject	spatial/temp.	no	yes	yes	yes
		resistance	no	no	no	yes
Social	Role	transitions	no	no	no	no
		interactions	no	yes	no	no

Table 1: Ability of the models to present digital/physical/social elements

From the presented results, we make the following observations. The ambient calculus is formal and capable of presenting most of the properties of interest. Other models impose restrictions on the model enabling them to focus on a specific area of interest, making the models less general than ambient calculus. This prevents the models to represent some of the properties of interest. TAM is incapable of presenting physical or social properties, because the model focuses on software representation and does not contain states. Scott and Dragovic cannot present role transition and role interaction because they do not include any social element in the model.

Table 2 provides an overview of the model's ability to present tampering with a physical device, the coldboot attack, as well as the road apple attack with indirect (road apple 1) and direct (road apple 2) interaction between the adversary and the user.

Name of attack	TAM & ST	Ambient calculus	Scott	Dragovic
Tampering	no	no	no	yes
Coldboot	partially	yes	yes	yes
Road apple 1	no	yes	yes	yes
Road apple 2	no	yes	no	no

Table 2: Ability of the models to present the case study attacks

Tampering with a device can be presented with the model of Dragovic because the model can contain information about the property of a device. TAM does not have this capability, and thus is not able to present the tampering. The model of Scott can use multiple layers to represent resistance, but the teleporting ability of data makes any attempt to represent resistance obsolete. The

operators in ambient calculus do not support teleporting, enabling the presentation of the tamper resistance through multiple layers. Yet, the capabilities of the ambient cannot change dynamically based on the change of the layer structure, preventing the complete presentation of tampering with data.

We are able to present the spatial movement of the dongle from the adversary to the employees laptop, but are not able to present the social interaction between the adversary and the user, where the adversary convinces the user to plug the dongle. This is the reason why Scott and Dragovic can only partially model the road apple with direct interaction.

5 Related work

Jiang et al. [18, 19] present a data structure for the privacy issues in the ubiquitous computing through data structures called *information spaces*. The model of Jiang et al. focuses on presenting social groups and activities, which is a major improvement with respect to the previously introduced security models, but the definition of the model is informal, making the model open for interpretation. Prayogi et al. [21] provide an access control framework for selective role transition based on the change of the context in which the system resides. Social and business fields have great interest in modeling user interaction, either for learning about their behavior or for generating policies that optimize profit [22].

6 Conclusion

We analyze the capability of state of the art security models to present the treats arising from mobility of data in dynamic organizations. We show that none of the state of the art security models simultaneously consider the data mobility and organizational dynamics to a satisfactory extent. Software modeling tools, like Microsoft's TAM, consider the physical infrastructure and roles to be static and this makes it hard to present dynamic changes in the system. Security models for ubiquitous computing are state based, but focus on spatial/temporal characteristics and fail to recognize social interactions, which are vital for social engineering threats. As a result, we conclude that none of the presented state of the art security models effectively identifies the potential security threats caused by data mobility in a dynamic organization.

The information omnipresence and dynamic organizations shift the stress from mainly digital attacks to a combination of digital, physical and social attacks. To cope with the threats, the paper presents the requirements for an integrated state based model. The goal of the proposed requirements is to aid in defining a model of the world from all three aspects, digital, physical and social and realistically present the possible attacks. The paper identifies the objects of interest from all three aspects and presents an initial classification of the properties affecting the security of the identified objects.

Future work is to define a formal security model that satisfies the requirements provided here and to define the interactions between the identified objects, based on the properties of the objects. An interesting direction is to use the properties of the objects presented in the model of Dragovic and extend it with roles to cover the social aspect of the world.

Acknowledgements

We thank Roel Wieringa, Siv Hilde Houmb, and André van Cleeff for their help with the paper. This research is supported by the Sentinels program of the Technology Foundation STW, applied science division of NWO and the technology programme of the Ministry of Economic Affairs under project number TIT.7628

References

Papers

[1] K.D. Mitnick and W.L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.

[2] D. Lacey. Inventing the future–the vision of the Jericho forum. *Information Security Technical Report*, 10:186–188, 2005.

[3] G. Palmer. De-perimeterisation: Benefits and limitations. *Information Security Technical Report*, 10:189–203, 2005.

[4] J. Walker. The extended security perimeter. *Information Security Technical Report*, 10:220–227, 2005.

[5] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik. Toward a threat model for storage systems. In *1st ACM Workshop on Storage Security and Survivability (StorageSS)*, pages 94–102. ACM Press, Nov 2005.

[6] L. Chen, D. Feng, and L. Ming. The security threats and corresponding measures to distributed storage systems. In *LNCS*, volume 4847, pages 551–559. Springer, 2007.

[7] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, and E.W. Felten. Lest we remember: Cold boot attacks on encryption keys. *USENIX Security*, pages 45–60, 2008.

[8] M. AlZarouni. The reality of risks from consented use of usb devices. In C. Valli and A. Woodward, editors, *Proceedings of the 4th Australian Information Security Conference*, pages 5–15, 2006.

[9] R. Wieringa. Conceptual modeling in social and physical contexts. Technical Report TR-CTIT-08-40, Centre for Telematics and Information Technology, University of Twente, 2008.

[10] F. B. Schneider. Enforceable security policies. *ACM Trans. on Information and System Security*, 3(1):30–50, Feb 2000.

[11] J. A. Goguen and J. Meseguer. Security policies and security models. In *3rd Symp. on Security and Privacy (S&P)*, pages 11–20. IEEE Computer Society, Apr 1982.

[12] L. Cardelli and A.D. Gordon. Mobile ambients. *Theoretical Computer Science*, 240(1):177–213, 2000.

[13] T. Dimkov, Q. Tang, and P. Hartel. On the inability of existing security models to cope with data mobility in dynamic organizations. Technical Report TR-CTIT-08-57, University of Twente, 2008.

[14] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Press Redmond, WA, USA, 2004.

[15] D.J. Scott. *Abstracting Application-Level Security Policy for Ubiquitous Computing*. PhD thesis, University of Cambridge, 2004.

[16] B. Dragovic and J. Crowcroft. Containment: from context awareness to contextual effects awareness. *2nd Intl Workshop on Software Aspects of Context (IWSAC'05)*, 2005.

[17] B. Dragovic and J. Crowcroft. Information exposure control through data manipulation for ubiquitous computing. In *NSPW '04: Proceedings of the 2004 workshop on New security paradigms*, pages 57–64. ACM, 2004.

[18] X. Jiang and J.A. Landay. Modeling privacy control in context-aware systems. *IEEE Pervasive Computing*, 1(3):59–63, 2002.

[19] X. Jiang, J.I. Hong, and J.A. Landay. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. *Proceedings of Ubicomp*, pages 176–193, 2002.

[20] P. Giorgini, H. Mouratidis, and N. Zannone. Modelling security and trust with secure tropos. *Integrating Security and Software Engineering: Advances and Future Vision*, pages 160–189, 2006.

[21] A.A. Prayogi, J. Park, and E. Hwang. Selective role assignment on dynamic location-based access control. *Convergence Information Technology, 2007. International Conference on*, pages 2136–2135, 21-23 Nov. 2007.

[22] W.R. Hartmann, P. Manchanda, H. Nair, M. Bothner, P. Dodds, D. Godes, K. Hosanagar, and C. Tucker. Modeling social interactions: Identification, empirical methods and policy implications. *Marketing Letters, forthcoming*, 2007.

Web references

[23] J. Ryder. Laptop security, part one: Preventing laptop theft. *SecurityFocus*, July 2001. http://www.securityfocus.com/infocus/1186.

[24] J. Ryder. Laptop security, part two: Preventing information loss. *SecurityFocus*, August 2001. http://www.securityfocus.com/infocus/1187.

[25] B. Rudis. Protecting road warriors: Managing security for mobile users , part one. http://www.securityfocus.com/infocus/1777, April 2004.

[26] B. Rudis. Protecting road warriors: Managing security for mobile users , part two. http://www.securityfocus.com/infocus/1781, May 2004.

[27] A. Shah. Analysis of rootkits: Attack approaches and detection mechanisms. http://www.cc.gatech.edu/~salkesh/files/RootkitsReport.pdf, 2006.

[28] S. Stasiukonis. Social engineering the usb way. http://www.darkreading.com/document.asp?doc_id=95556, 2006.

[29] Microsoft. Microsoft threat analysis and modeling v2.1.2. http://msdn.microsoft.com/en-us/security/aa570413.aspx, 2007.